confer
strength in numbers

WHITE PAPER

Achieving World-Class Security in Today's Cost-Conscious Business Climate

Bringing Real InfoSec to Regular Companies

About Confer

Confer developed the world's first cyberthreat prevention network that secures servers, laptops and mobile devices from advanced cyberattacks. Built on an open, wirespeed, threat-sharing platform, Confer enables companies to secure the enterprise with an intelligence-driven, threat-based defense, without requiring complex tools and deep security expertise.

Confer. Security that works.

Any casual observer of information security will tell you that the landscape has shifted dramatically in the last decade. In the '90s, we talked about "viruses" and "intruders." Today, we talk about "hacktivism," "cybercrime," "intellectual property theft," "espionage" and "cyberwarfare." We are dealing with a far more sophisticated adversary.

Meanwhile, the volume and breadth of the information we are trying to protect has grown by orders of magnitude. Not only is there more data to protect, it is spread out—both inside your corporate perimeter and elsewhere—across servers, laptops, mobile devices and in the cloud.

The old tools such as antivirus software that are still used for securing this information are failing. They are inherently reactive. They are complex and cumbersome. They lack visibility into attacks that take place on the road, at home, on mobile networks or in the cloud. All too often, they simply do not work.

High-end security practitioners have adjusted their approach and are changing the way we think about securing critical systems. In 2010, Lockheed Martin published an influential paper that defined the "kill chain," a useful model for looking at the complete lifecycle of an attack and strategically deploying controls and active, intelligence-driven defenses against those threats.[1] This model is illustrated in the following figure.

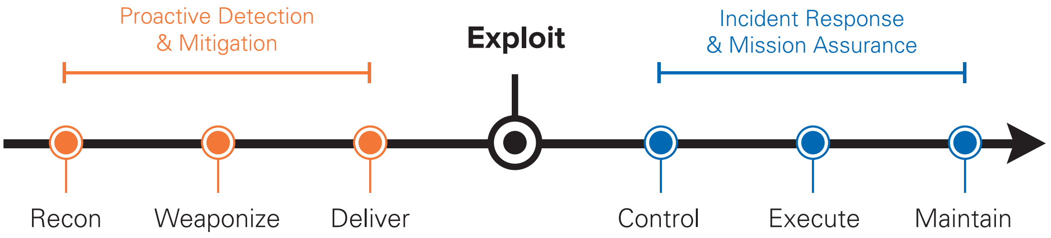


Figure 1: Kill Chain Model
Source: Confer

Recognizing the inherent value of the kill chain and its proactive approach to threat detection, many well-resourced security organizations—for example, within the defense and finance communities—are adopting an "active threat-based defense."

[1] Lockheed Martin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

They use the kill chain and other threat-based strategies to enable a more strategic approach to the problem and allow IT to break out of the endless detect-and-respond cycle that is so pervasive in the security space. They collect lots of information from across their infrastructure and analyze it to understand who is attacking them, what they are after and how and where in the kill chain they can best block them. In general, the earlier in the kill chain that we can detect, deny or disrupt our adversary—the better.

For most, though, this approach is too costly and complex. Previously, it has required considerable human capital to plan and execute an active threat-based security program. Security analysts are expensive and hard to find. This approach also requires a substantial financial investment to acquire and deploy the required sensors and controls.

Today, on average, security represents 5-10 percent of the overall IT budget but can range as high as 30 percent for a high-security operation. It simply is not realistic that security budgets will continue to grow.

Which raises the questions: How can we improve our defenses in a cost-sensitive business world? How can we move from a tactical, risk-based model to a strategic, threat-based model, without breaking the bank?

From Risk-Based to Threat-Based

Since the late '80s, the typical approach to security has been a risk-based one. In a risk-based model, you identify all the potential ways in which your company could be compromised and then either eliminate the vulnerability or deploy controls, i.e., firewalls, antivirus, IDS, etc., to prevent compromise.

This risk-based approach is not going away. In fact, it is the foundation for most compliance requirements. However, many question how effective this check-box approach is in preventing real attacks. In its January 2013 white paper on security, the Business Roundtable, an association of U.S. CEOs representing more than $7.3 trillion in annual revenues and nearly 16 million employees, quoted (right):

> **"[Compliance-based, check-the-box models] place the cart before the horse by calling for government creation of cybersecurity practices and standards… Ultimately, these compliance-based solutions would fail to create an adaptive and collaborative structure that would allow the public and private sectors to advance risk management models capable of managing cybersecurity threats as they continue to evolve."[2]**
>
> **More Intelligent, More Effective Cybersecurity Protection, Business Roundtable**

[2] Business Roundtable, "More Intelligent, More Effective Cybersecurity Protection," businessroundtable.org/uploads/studies-reports/downloads/More_Intelligent_More_Effective_Pre-Publication.pdf

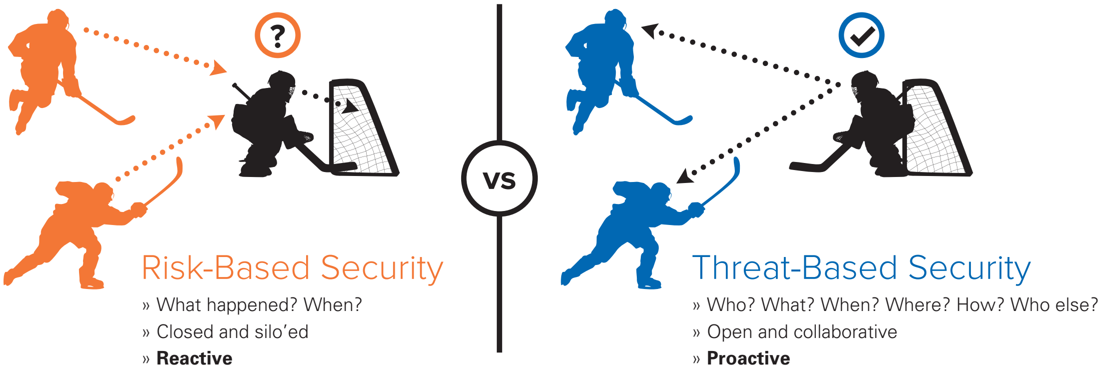


Figure 2: Threat-Based Security
Source: Confer

There are two fundamental issues with a pure risk-based approach:

1. **Despite our attempts to lock it down, the attack surface keeps expanding.** Every day, we are deploying more infrastructure, devices, software and operating systems. Security simply cannot keep up. It is like a game of whack-a-mole at the fair—as soon as you knock one down, another pops up.

2. **The fact is that not all threats are equal.** There is a wide spectrum of things we need to worry about, ranging from a "script-kiddie" to "espionage." A risk-based approach treats all threats the same way and focuses on the attack, not the attacker. With a risk-based approach, we are always playing defense and are hard-pressed to prioritize our response.

For these reasons, leading security organizations are attempting to transition to a strategic "threat-based" approach. In a threat-based model, we are just as concerned with the motivation and intent for an attack as we are the attack itself. In a threat-based model, we focus on:

- Who is being attacked?
- When and where did the attack come from?
- How did it get there?
- What were the attackers after?
- Were they successful?
- What was the business impact?
- Has this exploit been seen anywhere else?

And then, we prioritize the attack based on its potential business impact and respond accordingly. A threat-based model is inherently proactive. It arms IT organizations with a far better understanding of how and why they are attacked. In a threat-based model, we can learn and continuously improve.

Today, at organizations with large security teams, this is done by a team of highly-skilled security specialists, using an alphabet soup of expensive and complicated security products, i.e., SIM, IPS, DLP, sandboxing, etc., and external intelligence feeds. For many, this is simply too costly and complex, and they are stuck playing catch-up.

So, how can we enable a threat-based approach that is both effective and cost-efficient? We believe the answer lies in visibility and collaboration.

Threats Reveal Themselves on the Endpoint

The first challenge in a threat-based approach is to cost-effectively gather the information required to better understand the threat. Even well-resourced companies often lack visibility to their endpoints, one of the richest data sources for understanding the behavior of attackers.

Not all threats are equal. Endpoints hold the key to understanding each attack, identifying the degree of risk, and prioritizing our response. They provide insight into:

- Reconnaissance: Who is being targeted?
- Weaponization: What tools are being used to attack? Flash? PDFs? Has it been seen elsewhere?
- Delivery: What attack vectors (email, Web, etc.) are adversaries using?
- Exploitation: How effective are your preventative controls? Did anything get through? What data was accessed?
- Control and Exfiltration: Do you have active exploits in your company? What is the business impact?

Historically, we have largely relied on a combination of network-based inputs, i.e., firewall logs, IDS, etc., in attempting to answer these types of questions. However, these systems are costly, complex and often lack the visibility to get a comprehensive picture of the attack.

The endpoint is grossly underutilized as a security data source. The endpoint contains much of the context needed to understand who is being attacked, how and why. In the past, it has been cumbersome to gather this information from a distributed set of devices. However, with the emergence of pervasive networks, SaaS and cloud computing, it has recently become practical and cost-efficient to manage a large number of discrete endpoint sensors. By gathering this data and then analyzing it within the cloud, we can absorb, analyze and respond to far more information than has previously been possible.

Collaboration and Open Standards

The second challenge is to make sense of what we find. More specifically, how can we better identify and characterize the threats we face?

The security industry has traditionally employed a closed and proprietary model for threat identification and prevention. Typically, a security vendor builds a research team that tries to identify attacks. Information about these attacks is packaged into a proprietary signature feed that is delivered to a "black box." Hopefully this device blocks the bad stuff and lets the good stuff continue, but the customer rarely has a lot of input or visibility into how these decisions are made. Prior to 2005, this was largely how preventive security was done—and it is still the norm for many companies.

In recent years, better security teams are moving away from this model. Many security practitioners are sharing information and collaborating with a goal of better understanding the threats they face and developing an alternative, richer source of actionable security intelligence. Information Sharing and Analysis Centers (ISACs) have emerged and offer a community where security professionals can get a broader view of the threat landscape and advice on how to defend against advanced attackers. Companies are sharing more security information than ever before.

However, this is also a resource-intensive and complicated process. Threat information is shared via email, phone or chat groups. It is then manually massaged and entered—usually by scarce and expensive security analysts—into a variety of security products, such as IDS devices or firewalls.

This approach is inefficient and does not scale to the broad market. In response, MITRE Corporation has been developing a collection of technologies and standards—CRITs, STIX and TAXII—that facilitate automated sharing of threat information. STIX and TAXII are rapidly becoming the de facto standard for sharing threat information.

Confer[3] has collaborated with MITRE in the implementation of these standards and uses them across our product line.

The Collaborative Research into Threats (CRITs) solution combines a powerful security analytics engine with a cyberthreat database that not only serves as the main repository for attack data but also provides analysts with a platform for conducting their analysis.

[3] www.confer.net

These technologies allow us to build a more open and collaborative approach to securing our infrastructure. Specifically, they enable us to efficiently and automatically share information about the tactics, techniques and procedures (TTPs) used by attackers.

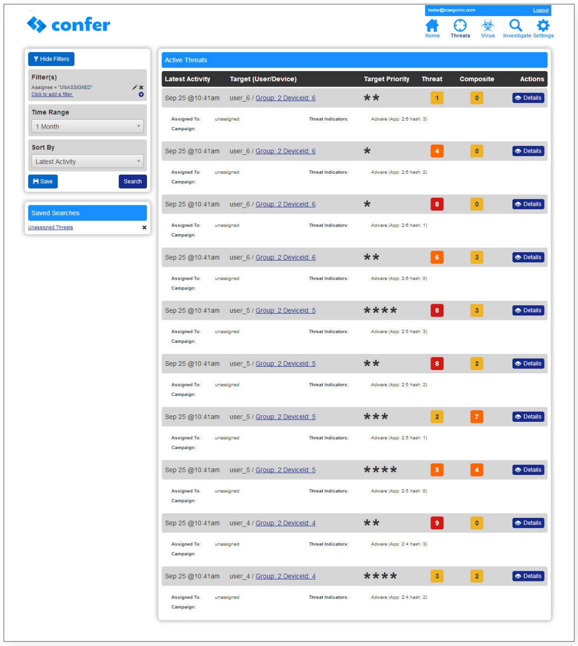
While legal departments are loath to share information about security incidents for privacy, regulatory or branding reasons, most companies can and often do share information about TTPs so that others can benefit. Identifiable information about the incident is stripped, while information about the attacker is shared.

Coupled with a well-defined security and privacy model that continuously protects proprietary data and personally identifiable information, this approach allows us to break the proprietary, black-box model typically employed in the security industry.

Confer: A Cyberthreat Prevention Network

Confer is the world's first open *cyberthreat prevention network,* an innovative proactive security service that protects servers, laptops and mobile devices from advanced cyberattacks. It is based on three principles:

- Security products should reduce work, not create more.
- Not all threats are equal.
- Companies should not "go it alone;" there is *strength in numbers.*



Filter(s)
Assignee = "UNASSIGNED"
Click to add a filter

Time Range: 1 Month

Sort By: Latest Activity

Active Threats

Latest Activity	Target (User/Device)	Target Priority	Threat	Composite	Actions
Sep 25 @10:41am	user_6 / Group: 2 DeviceId: 6	**	1	0	Details
Assigned To: unassigned Campaign:		Threat Indicators: Adware (App: 2:6 hash: 3)			
Sep 25 @10:41am	user_6 / Group: 2 DeviceId: 6	*	4	0	Details
Assigned To: unassigned Campaign:		Threat Indicators: Adware (App: 2:6 hash: 2)			
Sep 25 @10:41am	user_6 / Group: 2 DeviceId: 6	*	8	0	Details
Assigned To: unassigned Campaign:		Threat Indicators: Adware (App: 2:6 hash: 1)			
Sep 25 @10:41am	user_6 / Group: 2 DeviceId: 6	**	6	3	Details
Assigned To: unassigned Campaign:		Threat Indicators: Adware (App: 2:6 hash: 0)			
Sep 25 @10:41am	user_5 / Group: 2 DeviceId: 5	****	8	3	Details
Assigned To: unassigned Campaign:		Threat Indicators: Adware (App: 2:5 hash: 3)			
Sep 25 @10:41am	user_5 / Group: 2 DeviceId: 5	**	8	2	Details
Assigned To: unassigned Campaign:		Threat Indicators: Adware (App: 2:5 hash: 2)			
Sep 25 @10:41am	user_5 / Group: 2 DeviceId: 5	***	2	7	Details
Assigned To: unassigned Campaign:		Threat Indicators: Adware (App: 2:5 hash: 1)			
Sep 25 @10:41am	user_5 / Group: 2 DeviceId: 5	****	5	4	Details
Assigned To: unassigned Campaign:		Threat Indicators: Adware (App: 2:5 hash: 0)			
Sep 25 @10:41am	user_4 / Group: 2 DeviceId: 4	**	9	0	Details
Assigned To: unassigned Campaign:		Threat Indicators: Adware (App: 2:4 hash: 3)			
Sep 25 @10:41am	user_4 / Group: 2 DeviceId: 4	****	3	2	Details
Assigned To: unassigned Campaign:		Threat Indicators: Adware (App: 2:4 hash: 2)			

Screenshot 1: Proactive Detection of Advanced Threats
Source: Confer

Confer is easy to use and built on an open, threat-sharing community. It tells you how you are being attacked and what they are after. Since Confer protects the endpoint, you are always safe—at work, at home or on the road. Confer provides real, proactive, threat-based security to regular companies that have finite security budgets and limited security resources.

Confer Is Next-Generation Endpoint Protection

Confer continuously monitors your host system for the TTPs that attackers use—collecting and analyzing large volumes of TTPs in a secure cloud. What’s more, Confer gets ahead of attacks by capturing TTPs in advance—and then using this data to drive detection and provide insight into what happened. By applying advanced analytics, Confer looks for trends, pinpoints potential exploits and provides unprecedented visibility into the level of each threat and its impact on your business.

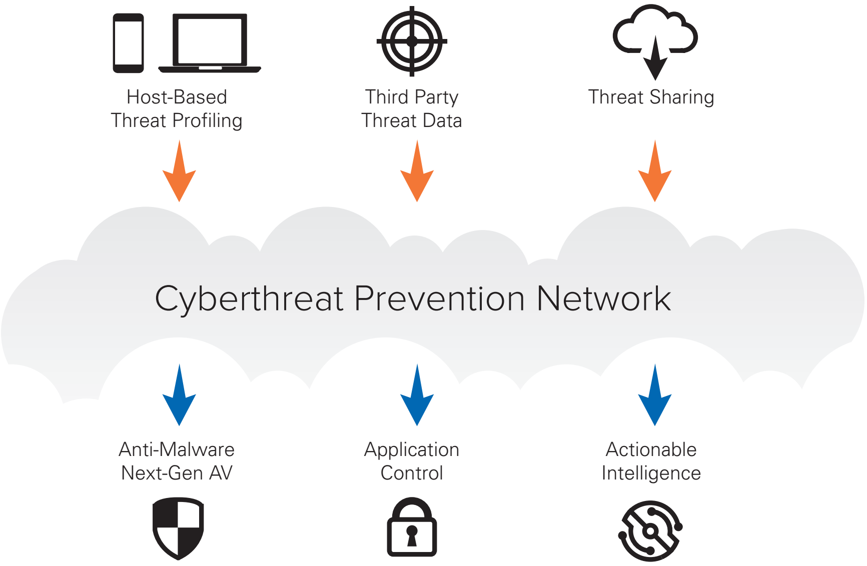


Figure 3: Cyberthreat Prevention Network
Source: Confer

Confer Is SaaS-Based and Easy to Deploy

Confer uses a lightweight, host-based sensor for Windows, Android and Mac-based systems. It installs in less than a minute and has no noticeable impact on system performance or battery life. Once installed, the service is completely managed from the cloud. All configuration, analysis and reporting is performed through an easy-to-use Web-based interface.

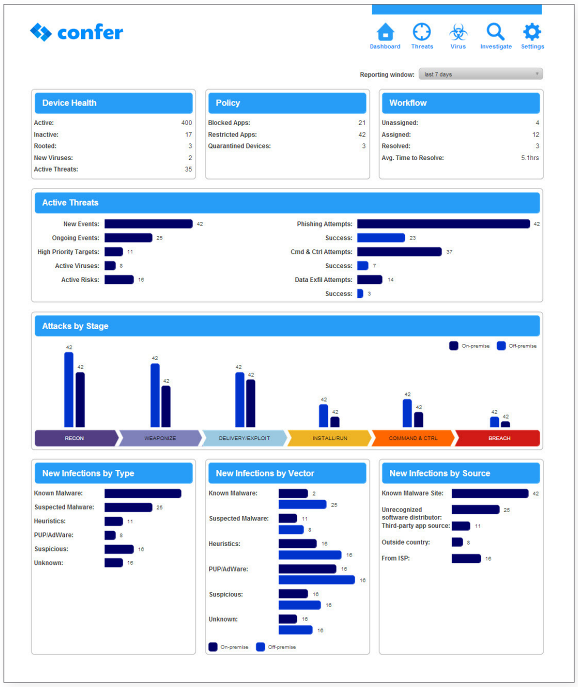
Confer Works from Anywhere

Since Confer is a cloud-managed, host-based system, it works from anywhere, not just from inside your network perimeter. It continuously monitors and protects endpoints regardless of where they are.

Confer Is Collaborative and Standards-Based

Confer is a community-based solution that shares information about threats. It gathers and analyzes TTPs from across the whole user base so that the instant one member identifies a threat, all members can benefit. Built on MITRE's widely-adopted STIX and TAXII standards for sharing threat data, Confer interoperates with other systems built on these standards.

Confer is working with FS-ISAC to ensure that the system can interoperate with their upcoming Avalanche product. Avalanche is a STIX- and TAXII-based threat repository. Confer will automatically consume indicators from Avalanche and apply them to the endpoint. Additionally, when Confer detects a new attack, it can export the details to Avalanche in STIX format to facilitate sharing with others.



Reporting window: last 7 days

Device Health	
Active:	400
Inactive:	17
Rooted:	3
New Viruses:	2
Active Threats:	35

Policy	
Blocked Apps:	21
Restricted Apps:	42
Quarantined Devices:	3

Workflow	
Unassigned:	4
Assigned:	12
Resolved:	3
Avg. Time to Resolve:	5.1hrs

Screenshot 2: Who, When, Where and How You Are Attacked
Source: Confer

Confer Provides Comprehensive Reporting and Integrated Search

Confer incorporates a built-in search engine to assist in pre- or post-attack analysis. Your administrator can instantly sort through the data, searching for untrusted applications and their associated TTPs across your company's entire infrastructure.

Confer also offers comprehensive reporting that provides broad visibility into your company's overall security posture, security trends and potential areas of exposure. The result? Management can better understand who is being attacked, where your business is most vulnerable and how to best allocate your security resources.

Summary

When it comes to mounting an effective response to today’s sophisticated cyberthreats, the winners will be those that deploy an active,threat-based defense – one that is broad and comprehensive, but also cost-efficient and simple to use. Confer’s collaborative, intelligence-based approach enables enterprises to substantially improve their threat awareness while protecting critical servers, laptops and mobile devices from advanced attackers.

At Confer, we don’t think enterprises should choose between world-class security and balancing the IT budget. With Confer, you don’t have to.

For More Information

Learn how you can take advantage of our free trial.
Visit www.confer.net today!

Author

Paul Morville
Founder and VP Products, Confer

confer
strength in numbers

Corporate Headquarters
950 Winter Street, Suite 4600
Waltham, MA 02451 USA

North American Sales
Toll Free 800.276.5180
sales@confer.net

www.confer.net